Java Security Issues and the New Java Segment Structure

April 05, 2002

Mike Ellis
michael.ellis@saic.com

SAIC
An Employee-Owned Company

Agenda

- **CRCB-approved risk management strategy for security vulnerabilities**
- **Current Java security vulnerabilities**
- **Affected Java Segments**
  - **Proposed versions for current JAVA 1 and JAVA2 segments to fix security issues**
- **New Java segment structure for Java 1.4 and higher**

CRCB-Approved Risk Management Strategy

- **Based upon a Java vulnerability, the CRCB approved a risk management strategy in May 2001 to migrate from vulnerable software versions**
- **Upon discovery of a Critical or Priority vulnerability for which no patch or workaround is expected:**
  - **COE Engineering Office will notify AOG that the vulnerable software version will be removed from the COE repository**
    - **Replaced with a new, secure version (if possible)**
    - **If removal will result in significant cost impact to the COE, CRCB will be consulted**
  - **System PMs will decide whether or not to continue using the vulnerable software version to support current operations**
- **Current Java security vulnerabilities warrant this risk management strategy**
  - **Need to separate JREs into individual segments in order to be able to migrate from vulnerable versions**

Java Security Issues

- **Recent Java Security Issues**
  - **Security Vulnerabilities in Java since March 4, 2002**
    - **Sun Security Bulletin #216 – Critical rating – COE vulnerability coe02_018**
      - **Allows an untrusted applet to monitor requests to and responses from an HTTP proxy server when a persistent connection is used between a client and an HTTP proxy server.**
    - **Sun Security Bulletin #217 – Routine rating – COE vulnerability coe02_024**
      - **A Java Web Start application may gain access to restricted resources.**
    - **Sun Security Bulletin #218 – Routine rating – COE vulnerability coe02_025**
      - **A vulnerability in the Java Runtime Environment Bytecode Verifier may be exploited by an untrusted applet to escalate privileges.**

Java Security Issues (2)

- **The following releases are affected by these Java security vulnerabilities:**
  - **Windows Production Releases**
    - **SDK and JRE 1.3.1_01a or earlier**
    - **SDK and JRE 1.3.0_05 or earlier**
    - **SDK and JRE 1.2.2_010 or earlier**
    - **JDK and JRE 1.1.8_008 or earlier**
  - **Solaris Production Releases**
    - **SDK and JRE 1.3.1_01 or earlier**
    - **SDK and JRE 1.3.0_05 or earlier**
    - **SDK and JRE 1.2.2_10 or earlier**
    - **JDK and JRE 1.1.8_14 or earlier**

JAVA1 Segment Versions

JAVA1 1.0.1.0 for Solaris	JAVA1 1.0.1.0 for Windows	JAVA1 1.0.1.0 for HP-UX 10.20
1.1.8_12	1.1.8_006	1.1.8_04
Proposed JRE versions in next JAVA1 Segments		
JAVA1 1.0.1.0 for Solaris	JAVA1 1.0.1.0 for Windows	JAVA1 1.0.1.0 for HP-UX 10.20
1.1.8_15	1.1.8_009	1.1.8_05
		Red = Vulnerable
		Green = Not Vulnerable

All are currently vulnerable !

JAVA2 Segment Versions

JAVA2 4.4.1.0 for Solaris	JAVA2 4.4.1.0 for Windows	JAVA2 4.4.1.0 for HP-UX 11.0
1.2.2_05a	1.2.2_006	1.2.2_004
1.2.2_010	1.2.2_010	1.2.2_006
1.3	1.3	1.2.2_010
1.3.1	1.3.1	1.3
1.3.1_01	1.3.1_01	1.3.1._02

All but one are vulnerable !

Proposed JRE versions in next JAVA2 Segments

JAVA2 4.4.2.0 for Solaris	JAVA2 4.4.2.0 for Windows	JAVA2 4.4.2.0 for HP-UX 11.0
1.2.2_011	1.2.2_011	1.2.2.011
1.3.1_03	1.3.1_03	1.3.1.02

Red = Vulnerable

Green = Not Vulnerable

New Java 1.4 JRE/SDK Segment Architecture

- ***Java JRE/SDK segment structures:***
  - **The new Java segments will contain only one version of Java (one JRE).**
    - **Enable better control over the Java segment (JRE management)**
      - Allowing COE community to remove JRE segments as the are OBE.
    - **The 64-bit optional package is specific to the JRE version**
    - **The JCE policy files is specific to the version of Java**
    - **Developers can add requires for the specific version they need.**
    - **Multiple versions can be installed on each platform**
    - **PostInstall is “smart” when it comes to installing OS patches and Font packages. If patches are already present they will not be installed, the same for Font packages.**

- **Issues with Java 1.4 and later to consider**
  - **32-bit and 64-bit versions**
  - **The Java JRE/SDK 1.4 now has 32-bit and 64bit support for Solaris 8. The main install is 32-bit and then the 64-bit supports comes in additional packages that are loaded later.**
    - **Recommend we have a 32-bit segment**
    - **Separate segment that adds the 64-bit additional files**

Java Cryptography Extensions

- **Java Cryptography Extension (JCE)**
  - **JCE 1.2.1 release became available. The primary difference between JCE 1.2 and JCE 1.2.1 is that JCE 1.2.1 is exportable outside the U.S. and Canada due to mechanisms it implements to ensure that only qualified providers can be plugged into the framework.**
  - **JCE has been integrated into the Java 2 JRE/SDK, v 1.4. Like JCE 1.2.1, it is exportable**
  - **The JCE framework in the Java 2 JRE/SDK, v 1.4 (and in JCE 1.2.1) includes an ability to enforce restrictions regarding the cryptographic algorithms and maximum cryptographic strengths available to applets/applications in different jurisdiction contexts (locations). Any such restrictions are to be specified in "jurisdiction policy files" that are downloaded along with the JCE software.**
  - **Due to import control restrictions of some countries, the jurisdiction policy files shipped with the Java 2 JRE/SDK, v 1.4 allow "strong" but limited cryptography to be used. An "unlimited strength" version of these files indicating no restrictions on cryptographic strengths is available.**
  - **Recommend that "unlimited strength" policy files be contained in a separate segment that can be export controlled.**

New Java JRE/SDK Segment Naming Convention

Java 2 Platform Standard Edition (J2SE) JRE

Segment Name	Segment Prefix	Directory Name	Version	Requires
J2SE JRE 1.4	J2JRE	J2JRE_1.4	4.6.0.0/1.4	None
J2SE JRE 64bit 1.4	J264RE	J2JRE_64bit_1.4	4.6.0.0/1.4	J2SE JRE 1.4
J2SE JRE JCE Policy 1.4	J2JCER	J2JRE_JCE_1.4	4.6.0.0/1.4	J2SE JRE 1.4

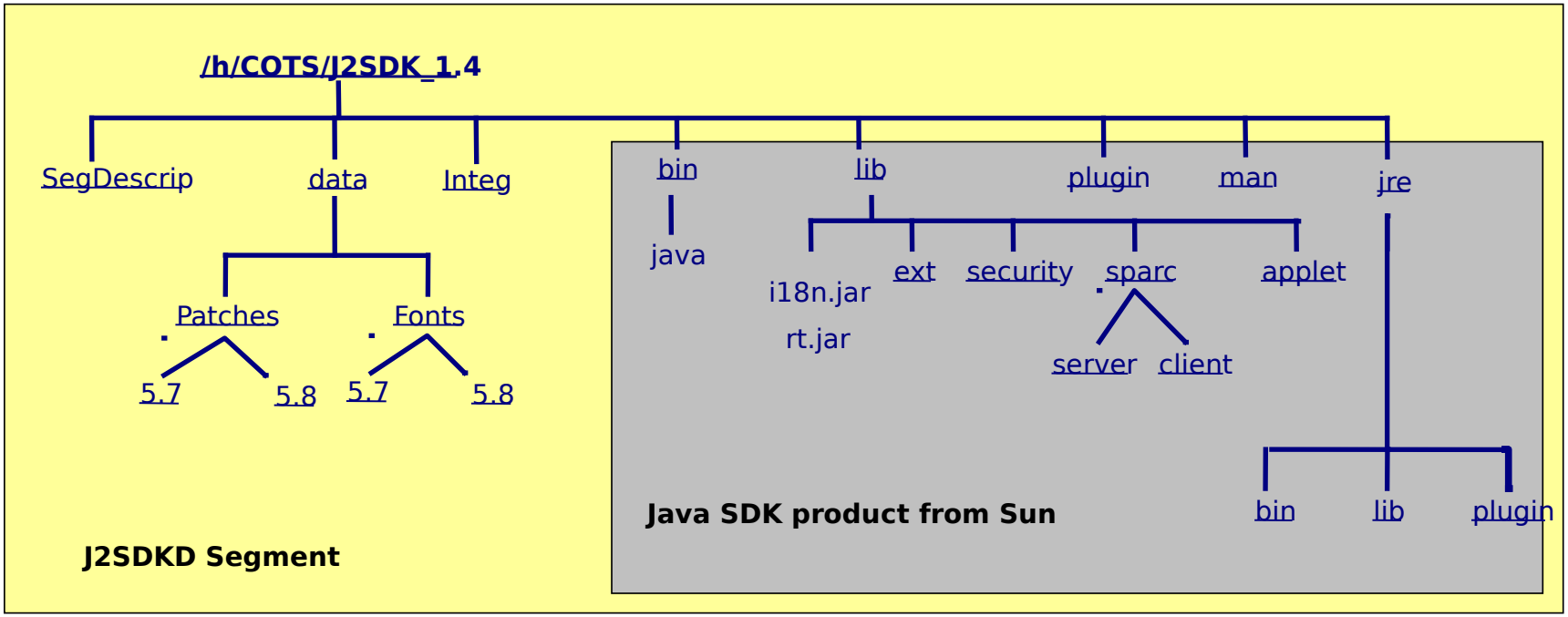
Java 2 Platform Standard Edition (J2SE) SDK

Segment Name	Segment Prefix	Directory Name	Version	Requires
J2SE SDK 1.4	J2SDK	J2SDK_1.4	4.6.0.0/1.4	None
J2SE SDK 64bit 1.4	J264SK	J2SDK_64bit_1.	4.6.0.0/1.4	J2SE SDK 1.4
J2SE SDK JCE Policy 1.4	J2JCEK	J2SDK_JCE_1.4	4.6.0.0/1.4	J2SE SDK 1.4

Example Requires Descriptor:

```
[Requires]
J2SE JRE 1.4:J2JRE:/h/COTS/J2JRE_1.4:4.6.0.0
```

J2SDK
Segment Directory Structure



Example segment structure